ALLEGATO A)

Azienda USL Toscana centro

REGOLAMENTO ATTUATIVO DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DI CUI AL D.LGS.30.06.2003 N° 196.

STATO DI REVISIONE

VER	N. ATTO	DATA	CAUSALE REVISIONE
00			
0			

PREMESSA

Il presente documento attuativo del Codice in materia di protezione dei dati personali di cui al D.Lgs. 196/03 e smi (di seguito denominato Codice) si inspira ai principi enunciati nel citato Codice, in particolare:

Diritto alla protezione dei dati personali – *(art. 1 D.Lgs 196/03 e smi)*

1.Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Finalità – *(art. 2 D.Lgs 196/03 e smi)*

1.Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonchè della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2.Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonchè per l'adempimento degli obblighi da parte dei titolari del trattamento

Principio di necessità nel trattamento dei dati *–(art. 3 D.Lgs 196/03 e smi)*

1.I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità

Il presente documento costituisce pertanto uno strumento di indirizzo e di politica aziendale in base al quale organizzare tutta l'azione necessaria ad assicurare la tutela del diritto alla riservatezza e la tutela dei dati personali e sensibili degli utenti.

Esso si propone inoltre l'obiettivo di concorrere al miglioramento della qualità dei percorsi di assistenza e di cura offerti ai cittadini, nell'ottica di garantire non solo la correttezza e la legalità dell'azione amministrativa, ma anche di promuovere il miglioramento continuo dei servizi erogati.

ART.1 – OGGETTO E AMBITO DI APPLICAZIONE

1. Il presente documento contiene disposizioni attuative del Codice da applicarsi all'interno dell'Azienda Unità Sanitaria Locale Toscana Centro, di seguito denominata Azienda. In particolare, esso intende fornire idonee istruzioni per l'applicazione del Codice nonché delle disposizioni emanate dal Garante per la Protezione dei dati personali (di seguito denominato Garante).

ART.2 – FINALITA'

1. La finalità del documento è quella di garantire che il trattamento dei dati personali da parte dell'Azienda avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda.

ART.3 – DEFINIZIONI

1. Nel presente documento e, comunque, in sede di trattamento dei dati personali, l'Azienda adotta le definizioni di cui all'articolo 4, comma 1, del Codice, con particolare riferimento a:

- **"trattamento",** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la

diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

- b) **"dato personale",** qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- c) **"dati identificativi",** i dati personali che permettono l'identificazione diretta dell'interessato;
- d**) "dati sensibili",** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- e**) "dati giudiziari",** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- f) **"dati comuni",** i dati personali non rientranti nella nozione di dati sensibili e dati giudiziari sono indicati di norma come dati comuni quali ad esempio nome e cognome, indirizzo , numero telefonico ecc.; tali dati "restano" comuni se non sono collegati ad un contesto di "sensibilità";
- g) **"titolare",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- h) **"responsabile"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- i) **"incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- l) **"interessato",** la persona fisica, cui si riferiscono i dati personali;
- m) **"comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- n) **"diffusione",** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- o) **"dato anonimo",** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- p) **"blocco",** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- q) **"banca di dati",** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- r) **"Garante",** l'autorità di cui all'articolo 153 del Codice.

2. Ai fini del presente documento sono, inoltre, adottate le seguenti ulteriori definizioni sulla base del Codice:

- a) **"misure minime",** il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- b**) "strumenti elettronici",** gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- c) **"autenticazione informatica",** l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

- d) **"credenziali di autenticazione"**, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;
- e) **"profilo di autorizzazione",** l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

ART.4 – ASPETTI DI POLITICA AZIENDALE

1. L'Azienda, nel perseguimento della propria missione di tutela della salute, tratta quotidianamente dati personali, di tipo "sensibile", dei propri cittadini-utenti. I dati personali idonei a rivelare lo stato di salute di un individuo sono infatti classificati dal Codice per la protezione dei dati personali entro la categoria dei dati "sensibili", in quanto attinenti alla sfera più intima della persona. Come tali, il legislatore ha previsto per essi una tutela rafforzata rispetto agli altri dati personali, cd "comuni".

2. Il rispetto del principio di riservatezza non costituisce soltanto un obbligo di legge che tutti gli operatori aziendali sono tenuti a garantire, con specifico riferimento al personale medico e sanitario, esso rappresenta, prima di tutto, un imperativo deontologico.

3. Nell'ipotesi di riordino del servizio sanitario regionale le disposizioni del presente regolamento in ordine alla profilatura della responsabilità privacy si adegueranno automaticamente, ove possibile e necessario, alla nuova organizzazione regionale.

ART.5 – PRINCIPI GENERALI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

1. Il *Codice* prescrive che i dati siano trattati nel rispetto dei seguenti principi:
- *liceità;*
- *legittimità;*
- *correttezza;*
- *finalità;*
- *proporzionalità e non eccedenza;*
- *necessità/indispensabilità;*
- *qualità.*

2. Il Codice all'art. 11 comma 1, lett. a) stabilisce che i dati personali devono essere *"trattati in modo lecito e secondo correttezza"*. I dati sono trattati **in modo lecito** se il trattamento rispetta:
- i presupposti e limiti stabiliti dal Codice, dalle leggi, dai regolamenti e dalle disposizioni del Garante;
- le eventuali disposizioni contenute nei codici di deontologia e di buona condotta di cui all'allegato A) del Codice;
- le misure minime di sicurezza di cui agli artt. 31-36 del Codice;
- le normative di settore (es. osservanza segreto professionale, rispetto della riservatezza in materia di interruzione della gravidanza o di tossicodipendenza o di soggetti HIV).

3**. La legittimità**, presuppone nel soggetto che effettua il trattamento un titolo valido ad assicurargliene la facoltà.

4. Il profilo della **correttezza del trattamento** (nella Direttiva *95/46/CE* si parlava di *lealtà*) richiama il più generale principio di buona fede e ricomprende anche la trasparenza nel comportamento del Titolare.

5. Il Codice all'art. 11 comma 1 b) stabilisce che i dati personali devono essere

- raccolti e registrati per **scopi determinati, espliciti e legittimi**, ed utilizzati in altre operazioni di trattamento in termini compatibili con tali scopi.

Per ogni trattamento occorre dunque una **finalità** determinata (cioè stabilita a priori), presente ed attuale (cioè tuttora valida), esplicita (cioè resa conoscibile) e lecita (nell'accezione sopra esaminata), la quale costituisce il parametro di riferimento per valutare i dati da trattare, sia in termini qualitativi che quantitativi. Le operazioni di trattamento non devono essere incompatibili con tali finalità (cd. **principio di finalità).** Un ente pubblico non può effettuare trattamenti che non rientrino tra le proprie finalità istituzionali. In particolare, per assicurare maggiori garanzie agli interessati, i trattamenti di dati sensibili e giudiziari effettuati da un ente pubblico sono leciti solo se riferibili a finalità di rilevante interesse pubblico individuate dalla legge.

6. I dati personali trattati devono essere, ai sensi dell'art. 11 comma 1 e) del Codice, conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
Quando la finalità è raggiunta o diviene irraggiungibile è necessario provvedere alla cancellazione o alla trasformazione in forma anonima dei dati, fatte salve le disposizioni in materia di archiviazione e conservazione dei documenti amministrativi. Ciò consente, tra l'altro, di prevenire possibili accessi abusivi ad informazioni non più attuali. E' considerato compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati l'ulteriore trattamento per fini storici, di ricerca scientifica o di statistica.

7. Un principio generale del sistema di garanzie approntato dal Codice è costituito dal principio di **pertinenza e non eccedenza,** integrato dal cd. **principio di necessità** con riferimento in particolare alla configurazione di sistemi informativi e programmi informatici.
I dati personali trattati devono dunque essere **pertinenti, completi e non eccedenti** rispetto alle finalità per le quali sono raccolti o successivamente trattati.
Il principio di **pertinenza e non eccedenza** sancisce l'obbligo di raccogliere solo i dati strettamente funzionali e necessari per il raggiungimento degli scopi legittimi perseguiti, completi e non eccessivi rispetto agli scopi stessi.
Il **principio di necessità** prevede invece che siano applicate ai dati modalità di trattamento che permettano di identificare l'interessato solo in caso di necessità. Il Codice prescrive (in particolare nei sistemi informativi e con i programmi informatici) all'art. 3 di trattare i dati :

- riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

8 Qualora il dato sia trattato da un soggetto pubblico, la norma richiede che siano trattati i soli dati essenziali per lo svolgimento delle attività istituzionali e che siano svolte le sole operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito.

9. Quando il trattamento riguardi dati sensibili, è legittimo solo l'utilizzo dei dati strettamente indispensabili.

10. I dati personali trattati, ai sensi dell'art. 11 comma 1 c) del *Codice*, devono essere infine (cd. **principio di qualità)** esatti e, se necessario, aggiornati.

ART.6 – IL DIRITTO ALL'AUTODETERMINAZIONE DELL'INTERESSATO AL TRATTAMENTO DEI DATI PERSONALI – INFORMATIVA E CONSENSO

1. L'Azienda garantisce il diritto dei cittadini-utenti all'autodeterminazione, fornendo un'informativa in possesso di tutti gli elementi previsti dall'art. 13 del Codice ed acquisendo preventivamente il consenso al trattamento dei dati personali per l'esecuzione delle attività di prevenzione, diagnosi, cura e riabilitazione, fatti salvi i casi di urgenza e le altre ipotesi di cui all'art. 82 del Codice nelle quali l'informativa e il consenso possono legittimamente intervenire dopo l'esecuzione della prestazione.

2.Il consenso costituisce una manifestazione di volontà libera, specifica ed informata con la quale la persona interessata accetta che i propri dati personali siano oggetto di un trattamento.
Il consenso autorizza l'Azienda all'effettuazione di tutti i trattamenti dati indispensabili all'erogazione delle prestazioni sanitarie richieste, sia per via cartacea, sia mediante i sistemi informatizzati.
Sebbene il consenso abbia natura facoltativa, l'eventuale diniego al trattamento impedisce l'erogazione delle prestazioni richieste e della risposta sanitaria (fatta eccezione per le prestazioni urgenti).

3. In conformità a quanto previsto dal Codice, il consenso al trattamento dei dati idonei a rivelare lo stato di salute può essere prestato anche verbalmente. In tal caso lo stesso è documentato, anziché con atto scritto dell'interessato, con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico.

ART.7 – IL DIRITTO ALL'ANONIMATO

1. L'Azienda garantisce, nell'ambito dei dati di cui all'elenco del seguente comma 2, l'adempimento dell'obbligo di un trattamento di dati non immediatamente identificativi del cittadino-utente, che si realizza, di norma, attraverso l'utilizzo di codici alfanumerici, che comunque il titolare, il responsabile, ovvero gli incaricati a ciò specificamente autorizzati (ai sensi dell'art. 85, comma 4, del Codice) hanno la possibilità di ricondurre ad un determinato soggetto.

2. Il trattamento dei dati relativi alle seguenti informazioni è sottoposto ad un regime normativo di particolare tutela:

- sieropositività;
- interruzione volontaria di gravidanza;
- vittime di violenza sessuale o di pedofilia;
- uso di sostanze stupefacenti, di sostanze psicotrope e di alcool ;
- parto in anonimato.

3.L'Azienda è impegnata a favorire fra gli operatori, l'adozione di comportamenti corretti improntati alla massima attenzione e cautela, nel trattamento dei sopracitati dati ipersensibili.

ART.8 – IL RISPETTO DEI CODICI DEONTOLOGICI

1. L'Azienda promuove il rispetto, da parte dei propri professionisti iscritti in albi professionali, delle disposizioni contenute nei rispettivi codici deontologici.
Qualunque trattamento di dati personali deve essere effettuato in ottemperanza a quanto in essi stabilito, pena la non liceità del trattamento stesso, ai sensi dell'art. 12, comma 3, del Codice.

ART.9 – LA VALUTAZIONE PREVENTIVA IMPATTO PRIVACY

1.L'Azienda, anche in considerazione dei principi delineati dalle disposizioni europee, assicura, nei casi in cui il trattamento, per la sua natura, il suo oggetto o le sue finalità, presenti rischi specifici per i diritti e le libertà degli interessati, una valutazione preventiva dell'impatto derivante sulla privacy degli interessati fin dalla progettazione del relativo processo aziendale.

2.Prima dell'avvio di un nuovo trattamento, in relazione a talune peculiari tipologie di dati e/o alle modalità di trattamento (ad esempio: attivazione di sistemi di videosorveglianza, trattamenti destinati alla prestazione di servizi sanitari, a ricerche epidemiologiche, indagini su malattie mentali o infettive qualora i dati siano trattati per prendere misure o decisioni su larga scala riguardanti persone specifiche, trattamento di dati biometrici) l'Azienda effettua pertanto un'analisi dei rischi in maniera tale da orientare le decisioni che verranno successivamente assunte verso soluzioni che siano effettivamente capaci di tutelare il dato già in sede di prima raccolta, con conseguente anticipazione di responsabilità alla fase di progettazione del trattamento stesso.

3. La valutazione d'impatto sulla protezione dei dati verte, in particolare, sulle misure di sicurezza, sulle garanzie e sui meccanismi previsti per assicurare la protezione dei dati personali e per comprovare il rispetto della normativa vigente in materia.

ART.10– LE POLITICHE DI ACCESSO AI DATA BASE E PROFILI DI AUTORIZZAZIONE

1. Nel rispetto del principio di necessità e pertinenza del trattamento dei dati personali, i profili di accesso ai programmi informatici aziendali sono configurati sulla base delle attività affidate a ciascun dipendente, e nel rispetto degli "ambiti di trattamento consentiti", così come individuati nel sistema aziendale privacy. L'assegnazione dei predetti profili ai singoli operatori incaricati del trattamento dei dati è effettuata a cura dei rispettivi responsabili del trattamento dei dati.

2. Per ciascuna banca dati (applicativo informatico) deve essere definito puntualmente l'elenco dei profili di accesso e le loro specificità.

3. Le finalità amministrative strettamente connesse all'erogazione della prestazione sanitaria (es. prenotazione e pagamento di una prestazione) devono essere realizzate garantendo il principio della necessità del trattamento, e quindi precludendo, per quanto possibile, l'accesso al personale amministrativo alle informazioni sanitarie, mediante la previsione di profili diversi di abilitazione in funzione della diversa tipologia di operazioni consentite.

4. In ogni caso gli accessi ai dati personali contenuti nei data base aziendali devono essere ridotti allo stretto necessario per consentire l'espletamento delle ordinarie attività lavorative. Il trattamento dei dati deve, pertanto, essere evitato ogni volta in cui lo stesso non sia indispensabile per il perseguimento degli scopi prefissati.

5. Periodicamente e, comunque, almeno una volta all'anno, i responsabili del trattamento aggiornano i profili di autorizzazione del personale assegnato.

6.Al fine di garantire che il trattamento dei dati inerenti allo stato di salute degli utenti sia effettuato con un idoneo livello di sicurezza, gli accessi ai software clinici devono essere tracciati.

ART.11 – LA COMUNICAZIONE DI DATI A TERZI

1. L'Azienda effettua la comunicazione di dati personali a terzi, pubblici e privati, solo in conformità a quanto previsto dalle vigenti disposizioni legislative e regolamentari in materia.
Anche nell'ipotesi in cui la comunicazione sia espressamente consentita da specifica disposizione di legge o di regolamento, l'Azienda evita il trattamento dei dati personali quando le finalità da perseguire nei singoli casi possono essere realizzate anche mediante l'utilizzo di dati anonimi o ricorrendo ad opportune tecniche di crittografia.

ART.12 – TITOLARE DEL TRATTAMENTO DEI DATI

1. Il Titolare del trattamento dei dati personali ai sensi e per gli effetti del Codice è l'Azienda USL Toscana Centro.

2. Il Titolare avvalendosi del Referente Aziendale privacy (di seguito denominato RAP), al quale dovranno essere fornite idonee ed adeguate risorse umane e strumentali, del Referente Informatico per la protezione dei dati (di seguito denominato RIPD) provvede nei casi e nelle forme previste dalle legge e dal presente regolamento:

- ad assolvere all'obbligo di notificazione al Garante per la protezione dei dati personali previsto dall'art. 37 del Codice e nelle situazioni previste dal successivo art. 18, nonché all'obbligo delle comunicazioni al Garante stesso previste dall'articolo 39, comma 1, del Codice;
- a richiedere al Garante l'autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa;
- a definire e disporre, le misure necessarie a garantire la conservazione, la protezione e la sicurezza dei dati personali;
- a nominare con proprio atto i responsabili del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'articolo 7 del Codice, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
- a individuare le risorse umane di cui al presente comma 2, di provata competenza in materia di protezione del dato sia in ambito giuridico che informatico, anche in considerazione dell'esponenziale crescita della digitalizzazione in sanità;
- a disporre periodiche verifiche nei confronti dei responsabili del trattamento, sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati.

ART.14 – RESPONSABILE DEL TRATTAMENTO DEI DATI

1. Il Titolare designa con atto formale i Responsabili del trattamento dei dati (più oltre indicati "responsabili del trattamento") fra i soggetti che, come disciplinato all'art. 29, comma 2, del Codice, per esperienza, capacità ed affidabilità, forniscono idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di riservatezza, ivi compreso il profilo relativo alla sicurezza.

2. Il Titolare individua quali responsabili del trattamento, nell'attuale assetto organizzativo e per i trattamenti dei dati in relazione alle funzioni di specifica competenza:

- Direttore Amministrativo;
- Direttore Sanitario;
- Responsabili Dipartimentali;

- Responsabili di Area;
- Responsabili delle strutture organizzative

3. Fermo restando quanto previsto al precedente comma 2, per i trattamenti che non si esauriscono all'interno di una singola struttura organizzativa ma interessano strutture diverse o livelli generali di organizzazione, è nominato Responsabile del trattamento il Responsabile della struttura che, nell'ambito del trattamento nel suo complesso, ha la componente maggioritaria per trattamento di dati e per livello di responsabilità.

4. Il Titolare può, inoltre, individuare quali responsabili del trattamento, altri soggetti (dirigenti/funzionari/titolari di incarichi) in virtù delle particolarità organizzative e funzionali delle attività di competenza.

5. Il dipendente che svolge attività libero professionale intramuraria è individuato quale Responsabile del trattamento dei dati effettuati in tale attività.

6. La struttura competente in merito alla gestione dell'attività libero-professionale intramuraria (ALPI) deve inserire nell' autorizzazione a tale attività, l'atto di designazione a responsabile del trattamento del dipendente interessato.

7. Il Responsabile del trattamento di cui al precedente comma 5, deve provvedere, se necessario, a designare ai sensi dell'art. 16 del presente regolamento gli incaricati (personale di supporto all'ALPI) del trattamento dati e fornire loro specifiche istruzioni.

8. Nell'ambito degli studi osservazionali/ sperimentazioni, attivati in Azienda è individuato quale responsabile del trattamento il singolo professionista debitamente autorizzato alla realizzazione dello studio/sperimentazione.

9. La funzione di responsabile non è delegabile. In caso di assenza o impedimento del responsabile del trattamento, le relative attribuzioni sono esercitate da chi lo sostituisce per le attività di istituto.

10. I Responsabili del trattamento svolgono i seguenti compiti, direttamente o avvalendosi dei soggetti di cui all'art. 16:

- applicare la normativa contenuta nel Codice, le disposizioni del Garante, le disposizioni contenute nel presente regolamento, nonché la normativa nazionale e regionale che disciplina specifici trattamenti di dati;
- osservare le istruzioni impartite dal Titolare vigilando sull'applicazione delle stesse;
- individuare adeguate misure organizzative e gestionali dirette ad assicurare a tutti i soggetti interessati il diritto alla riservatezza ed alla protezione dei dati personali;
- verificare che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza, che i profili di autorizzazione degli incaricati al trattamento dei dati afferenti al responsabile stesso, rispondano ai principi di necessità, pertinenza e non eccedenza;
- verificare che il trattamento sia coerente con le funzioni istituzionali dell'Azienda e che le stesse finalità non siano perseguibili attraverso il trattamento di dati non identificativi o anonimi;
- verificare che all'interessato o al soggetto presso il quale sono raccolti i dati sia data l'informativa di cui all'art.13 del Codice;
- verificare che l'interessato o altro soggetto legittimato presti, quando previsto, il consenso al trattamento dei dati;
- verificare che il personale assegnato sia designato incaricato del trattamento, fornendo le specifiche istruzioni;

- rispondere alle istanze degli interessati secondo quanto stabilito dal Codice, attenendosi alle disposizioni di cui all'art. 40 del presente Regolamento, e predisponendo modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato;
- ricevere e valutare le richieste di accesso ai documenti amministrativi, avanzate ai sensi dell'art. 22 della Legge 241/1990 e smi, attenendosi alle disposizioni di cui all'art. 41 del presente Regolamento;
- ricevere e valutare le richieste di accesso civico generalizzato, avanzate ai sensi del D.Lgs 33/2013 e smi, di cui all'art.42 del presente Regolamento;
- fornire al Garante le informazioni richieste, consentire i controlli e gli accessi da parte delle autorità competenti;
- ottemperare ad ogni altro adempimento stabilito dal Titolare in relazione al trattamento dei dati personali.

Collaborare con il RAP nell'espletamento dei suoi compiti, in particolare al fine di:

- comunicargli tempestivamente l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto anche ai fini dell'eventuale variazione della notifica al Garante, nonché ogni notizia rilevante ai fini della tutela della sicurezza e riservatezza dei dati personali;
- segnalargli i casi in cui a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi come incendi o altre calamità, si dovessero verificare la perdita, la distruzione o la diffusione indebita di dati personali trattati nel rispetto dei provvedimenti del Garante (cd. "data-breach");
- fornirgli gli elementi informativi necessari per effettuare le comunicazioni di cui all'articolo 39, comma 1, del Codice;
- fornirgli le informazioni necessarie per l'aggiornamento degli archivi di cui all'art.18, lettera c) ed ogni altra informazione richiesta per l'attuazione del presente Regolamento;

11. Ogni modifica di responsabilità delle strutture organizzative afferenti al Responsabile del Trattamento deve essere segnalata al RAP .
La struttura deputata alla gestione delle risorse umane dovrà provvedere alla predisposizione degli atti di designazione a responsabile del trattamento contestualmente all'assegnazione dell'incarico nell'ambito dell'organizzazione aziendale, utilizzando gli specifici format aziendali in sede di sottoscrizione del contratto individuale.

12. Possono essere individuati, quali responsabili del trattamento, con le modalità previste all'art. 15, soggetti esterni all'Azienda, in caso di fornitura di procedure complesse anche di natura informatica o telematica, di prestazioni professionali, o di prestazioni e servizi anche in convenzione.

13. I Responsabili del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla vigente normativa e dalle istruzioni ricevute, ivi comprese quelle riguardanti l'adozione delle misure di sicurezza.

ART.15 – RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

1. I soggetti che, per esigenze organizzative dell'Azienda e in funzione del perseguimento dei suoi fini istituzionali e in base a uno specifico rapporto giuridico, effettuano con utilizzazione della propria organizzazione o di quella dell'Azienda stessa trattamenti di dati per conto di quest'ultima, sono designati responsabili esterni del trattamento, sempre che in possesso dei requisiti previsti dall'articolo 29, comma 1, del Codice (esperienza, capacità, affidabilità).

2. La designazione a responsabile esterno del trattamento è effettuata dal Titolare. A tal fine le strutture aziendali che stipulano convenzioni o contratti con soggetti esterni all'Azienda devono compilare lo schema dell'atto di nomina a responsabile esterno del trattamento allegandolo alla

deliberazione con la quale si approva lo schema di contratto e/o convenzione. L'atto di designazione sarà perfezionato contestualmente alla sottoscrizione del contratto e/o convenzione.

3. La sottoscrizione della designazione e l'impegno a rispettare le disposizioni previste dal presente regolamento è condizione essenziale per l'inizio dello specifico rapporto giuridico tra le parti. E' fatto obbligo alla struttura competente per la stipula del contratto o della convenzione trasmettere al RAP entro sette giorni dalla stipula, copia dell'atto di designazione del responsabile esterno controfirmato per accettazione, nonché provvedere alla consegna (anche con informazione sulla possibilità di consultarlo via web sul sito istituzionale) del presente regolamento ai soggetti firmatari del contratto o della convenzione.

4. Nei contratti di affidamento di attività o di servizi all'esterno dell'Azienda (outsourcing) è inserita apposita clausola di garanzia con cui il soggetto affidatario, individuato responsabile esterno del trattamento dei dati, si impegna, nel trattamento dei dati personali effettuati in forza del rapporto contrattuale, all'osservanza delle norme del Codice e di quanto disposto dall'Azienda in materia ai sensi degli artt. 20, 21 e 22. Il responsabile esterno del trattamento, in particolare, si impegna a:

- effettuare il trattamento dei dati in modo lecito e corretto, nei limiti dei compiti affidati e nel rispetto della normativa vigente;
- assumere le misure necessarie per evitare rischi di distruzione o perdita anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- non effettuare operazioni di comunicazione o diffusione dei dati trattati qualora non previste da norme di legge o di regolamento;
- accedere ai dati patrimonio del Titolare, esclusivamente in funzione dell'espletamento dei propri compiti e delle attività esternalizzate;
- segnalare i casi in cui a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi come incendi o altre calamità, si dovessero verificare la perdita, la distruzione o la diffusione indebita di dati personali trattati nel rispetto dei provvedimenti del Garante (cd. "data-breach");
- comunicare al Titolare le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali;
- comunicare i luoghi ove fisicamente avviene il trattamento dei dati e su quali supporti;
- fornire in ogni momento le informazioni richieste e segnalare ogni questione rilevante ai fini dell'applicazione della normativa in materia di protezione dei dati;
- nominare per iscritto gli incaricati del trattamento fornendo loro le necessarie istruzioni e provvedere alla trasmissione dell'elenco degli incaricati designati al Titolare.

Inoltre, qualora tra le attività oggetto del contratto/convenzione rientrino quelle funzioni proprie dei cd. Amministratori di sistema di cui al provvedimento del Garante del 27/11/2008 deve essere integrata la suddetta clausola con il seguente testo:

- il responsabile esterno del trattamento dei dati si impegna ad osservare le disposizioni del Garante in materia di Amministratori di Sistema conservando direttamente e specificatamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema fornendo il relativo elenco al Titolare.

5. Il Responsabile esterno risponde dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi degli artt. 1218 e 1223 del Codice Civile.

6.Le strutture aziendali competenti nella gestione del contratto o convenzione devono provvedere all'applicazione di quanto disciplinato nel presente regolamento, adeguando, se necessario, anche mediante apposito atto aggiuntivo, i contratti o convenzioni in essere ai sensi del presente regolamento e della normativa vigente, devono, altresì, provvedere ad inviare al RAP gli atti di designazione a responsabile esterno del trattamento dei dati.

ART.16 – INCARICATI DEL TRATTAMENTO DEI DATI

1. Gli incaricati del trattamento dei dati, ai sensi dell'art.30 del Codice, sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o responsabile.

2. Il Responsabile del trattamento verifica che il personale assegnato sia designato incaricato a svolgere le operazioni di trattamento dei dati personali di competenza precisando, con riferimento alle istruzioni ricevute dal Titolare, i relativi compiti, l'ambito del trattamento consentito e le modalità cui devono attenersi.

3. La designazione degli incaricati è effettuata con atto scritto. L'atto di nomina costituisce presupposto di liceità per il trattamento dei dati personali.

4. La designazione di cui al precedente comma 3, e le modalità e l'ambito cui deve attenersi l'incaricato, ai sensi dell'art.30, comma 2, del Codice può essere effettuata anche tramite la formale assegnazione di un incaricato ad una struttura organizzativa o ad una funzione con indicazioni di idonee ed adeguate istruzioni. Nel caso di soggetti per i quali non si possa fare riferimento ad una formale assegnazione dovrà essere predisposto uno specifico atto di designazione da parte del responsabile del trattamento.

5. Gli incaricati hanno accesso ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti istituzionali loro assegnati.

6. Durante il trattamento od in caso di allontanamento dal posto di lavoro, l'incaricato deve adottare le misure previste e a sua disposizione, secondo le istruzioni ricevute dal responsabile del trattamento, per evitare l'accesso non autorizzato da parte di terzi, anche se dipendenti, ai dati personali trattati o in trattamento.

7. Ai sensi dell'art.83, comma 2, del Codice anche gli incaricati del trattamento che non sono tenuti per legge al segreto professionale, sono sottoposti a regole di condotta analoghe al segreto professionale.

8. L'Azienda prevede annualmente interventi formativi degli incaricati del trattamento dei dati al fine di consentire l'acquisizione di comportamenti metodologicamente corretti in materia di riservatezza e di protezione dei dati.

ART.17 – OBBLIGHI DELLE PERSONE CHE OPERANO ALL'INTERNO DELL'AZIENDA

1. Tutte le persone che funzionalmente svolgono operazioni di trattamento su dati di cui l'Azienda ha la titolarità, nonché prestano attività all'interno dell'Azienda stessa a qualsiasi titolo, con o senza retribuzione, compresi gli allievi e i docenti dei corsi di formazione e di aggiornamento professionale, anche in convenzione con le università, gli specializzandi, i tirocinanti e i volontari, qualora in occasione della loro attività vengano a conoscenza di dati personali trattati dall'Azienda sono designati, dai relativi responsabili del trattamento, quali incaricati esterni del trattamento dei dati estendendo a tali designazioni quanto disciplinato all'art.16 del presente regolamento.

2. Per le finalità di cui al precedente comma, il Responsabile del trattamento fornisce le necessarie informazioni alle persone che operano a qualsiasi titolo nella propria struttura.

ART.18 –IL REFERENTE AZIENDALE PRIVACY

1. Il Titolare del trattamento dei dati designa con atto formale, il Referente Aziendale Privacy (RAP) individuato tra il personale dipendente con idonea posizione funzionale.

2. Il RAP si avvale della collaborazione del Referente Informatico Privacy di cui al successivo art. 19 per la stesura del Documento Aziendale per la Sicurezza in materia di privacy e per l'assolvimento degli adempimenti in materia di privacy in relazione alla specifica competenza.

3. Il RAP al quale devono essere assegnate risorse umane e strumentali idonee e adeguate, svolge i seguenti compiti:

a. informa e fornisce consulenza al Titolare, ai Responsabili del trattamento, per quanto riguarda gli adempimenti derivanti dalla normativa in materia di riservatezza e protezione dei dati personali;
b. fornisce, dietro richiesta, un parere in merito alla valutazione d'impatto sulla protezione dei dati;
c. tiene i rapporti con il Garante;
d. sorveglia l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati Membri relative alla protezione dei dati nonché delle politiche del Titolare in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al trattamento ed alle connesse attività di controllo;
e. cura la costituzione e l'aggiornamento degli archivi sottospecificati, sulla base dei dati forniti dai responsabili del trattamento, nonché dalla struttura deputata alla gestione delle risorse umane, i quali hanno la piena e completa responsabilità in merito a informazioni di dati deficitari o totalmente mancanti:
   - censimento dei trattamenti dei dati personali (Ce.Tra);
   - elenco dei responsabili dei trattamenti, anche esterni, con i relativi recapiti;
   - elenco degli archivi cartacei con indicazione delle rispettive sedi e caratteristiche;
   - elenco delle banche dati personali informatiche custodite dall'Azienda, con indicazione delle rispettive sedi e caratteristiche fornito dal RIPD ai sensi dell'art.19,comma 2 lettera e.;
f. effettua i necessari approfondimenti per l'applicazione della normativa in materia di protezione dei dati personali, anche mediante la costituzione di appositi gruppi di lavoro;
e. cura l'attivazione di flussi informativi, utilizzando il sistema di rete aziendale, con modalità adeguate tali da fornire uno strumento on line di informazione e conoscenza, rivolto ai Responsabili/incaricati del trattamento dei dati personali al fine di promuovere un'azione di sensibilizzazione in materia di riservatezza;

4. L'Azienda assicura al RAP adeguate ed idonee risorse, strumentali, informatiche ed umane, nonché garantisce l'apporto di tutte le strutture organizzative per lo svolgimento dei compiti ad esso assegnati.

ART.19 – IL REFERENTE INFORMATICO PROTEZIONE DEI DATI

1. Il Titolare del trattamento dei dati nomina con atto formale, il Referente Informatico per la protezione dei dati (RIPD) scelto tra il personale dipendente con idonea posizione funzionale.

2. Il Referente Informatico per la protezione dei dati svolge i seguenti compiti:

a. collabora con il RAP nell'assolvimento delle funzioni sulla base di quanto di competenza;

b. predispone la relazione in merito agli aspetti della sicurezza informatica dei trattamenti con strumenti elettronici che costituisce parte integrante del Documento Aziendale per la Sicurezza in materia di privacy;
c. fornisce, dietro richiesta, un parere in merito alla valutazione d'impatto sulla protezione dei dati;
d. cura i rapporti con il soggetto al quale l'Azienda ha affidato la gestione delle reti informative e delle tecnologie informatiche, al fine di garantire che le procedure informatiche siano conformi alla normativa in materia di protezione dei dati personali;
e. cura la tenuta dell' elenco delle banche dati informatiche custodite dall'Azienda, con indicazione delle rispettive sedi e caratteristiche;
f. cura la tenuta dell'elenco dei soggetti abilitati a ciascun applicativo secondo i profili di autorizzazione istituiti.

ART.20 – AMMINISTRATORI DI SISTEMA

1. Per Amministratore di Sistema, ai sensi del Provvedimento del Garante del 27/11/2008 come modificato con provvedimento del 25/06/2009, si intende la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con i quali vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza nella misura in cui consentano di intervenire sui dati personali.

2. Rientrano nell'accezione ampia di cui al precedente comma 1, una serie di figure chiamate a svolgere funzioni che comportano la concreta capacità di accedere, in modo privilegiato, a risorse del sistema informativo e ai dati personali e nella misura in cui sono, nelle loro consuete attività tecniche, responsabili di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:

- gestione dei sistemi di autenticazione e di autorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- salvataggio dei dati (backup/recovery);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- manutenzione hardware

3. Possono qualificarsi quale Amministratori di sistema i seguenti soggetti:

- amministratori di sistemi di autenticazione e di autorizzazione;
- amministratori di server;
- amministratori di apparati di rete;
- amministratori di base di dati;
- amministratori di apparati di sicurezza;
- amministratori di applicazioni.

4. Non rientrano nella definizione di cui sopra quei soggetti che solo occasionalmente intervengono sui sistemi di elaborazione e sui sistemi software.

5. I soggetti di cui al precedente comma 3 devono essere designati nominativamente con puntuale ed analitica indicazione dei compiti assegnati.

6.Qualora l'attività degli amministratori di sistema riguardi servizi o sistemi che trattano informazioni di carattere personale di dipendenti, l'Azienda è tenuta a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito della propria organizzazione.

7. Nel caso di servizi di amministrazione di sistema affidati in outsourcing, e in base alla organizzazione regionale di cui alla L.R.T. n. 26/2014 di istituzione dell'ESTAR, il fornitore del servizio – da individuarsi con le modalità ed i criteri di cui al precedente art. 15, quale Responsabile esterno del trattamento dei dati – è tenuto, in particolare, a:

- precisare analiticamente per ciascun soggetto designato quale amministratore di sistema l'ambito di operatività consentito in base al profilo di autorizzazione assegnato;
- conservare e aggiornare direttamente e specificatamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;
- verificare l'operato degli amministratori;
- adottare sistemi di registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori.

ART.21 – LE MISURE MINIME DI SICUREZZA

1. Per il trattamento dei dati personali, l'Azienda, adotta misure di sicurezza, fisiche, logiche ed organizzative - di cui al disciplinare tecnico in materia di misure minime di sicurezza, allegato B) al Codice - al fine di garantire l'integrità, la disponibilità e la protezione dei dati stessi e di ridurne al minimo i rischi di distruzione o perdita, anche accidentale, e di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

2. Per la realizzazione delle finalità di cui al comma 1, si provvede anche con la predisposizione di apposite policy alle quali viene data ampia diffusione nei confronti dei responsabili/incaricati del trattamento.

3. Tutti i responsabili del trattamento interni ed esterni sono tenuti ad adottare le misure di sicurezza ulteriori rispetto a quelle minime previste dalla normativa vigente che si rendessero necessarie in relazione alle specifiche esigenze della struttura gestita, tenuto conto del livello di esposizione al rischio cui sono soggette le attività di trattamento dati affidate, della peculiarità e delicatezza dei trattamenti dati effettuati, nonché dello sviluppo tecnologico.

4. L'adozione delle misure minime è condizione di legittimità del relativo trattamento: ciò significa che un trattamento eseguito senza che siano adottate le relative misure minime di sicurezza è illegittimo.

ART.22 – MISURE MINIME DI SICUREZZA INFORMATICA

1. Il trattamento di dati personali con l'ausilio di strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione.

2. I profili di autorizzazione, per ciascuno incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

3. Ulteriori istruzioni organizzative e tecniche per la custodia e l'utilizzo degli strumenti e delle tecnologie informatiche sono impartite con specifici documenti (policy etc..) o con procedure operative.

ART.23 – MISURE DI SICUREZZA DEGLI ARCHIVI CARTACEI

1. L'accesso agli archivi aziendali contenenti dati personali di tipo sensibile e giudiziario deve essere controllato mediante l'accertamento dell'identità del soggetto che vi accede. Qualora gli archivi non dispongono di strumenti elettronici per il controllo degli accessi o di incaricati per la vigilanza, le persone che vi accedono devono essere preventivamente autorizzate; le persone autorizzate che vi accedono dopo l'orario di chiusura devono comunque essere identificate e registrate.

2. La responsabilità della conservazione e della sicurezza degli archivi cartacei di uso corrente, contenenti dati personali spetta al responsabile del trattamento di tali dati.

3. La responsabilità dei trattamenti correlati alla gestione dell'archivio di deposito è attribuita al soggetto esterno aggiudicatario del servizio di archiviazione.

ART.24 – MODALITA' DI TRATTAMENTO DI DATI PERSONALI

1. Il trattamento dei dati personali è ammesso solo da parte del titolare del trattamento, dei responsabili e degli incaricati. Non è consentito il trattamento di dati personali da parte di persone non autorizzate.

2. Il trattamento dei dati personali raccolti direttamente dall'Azienda o ad essa comunicati da altri soggetti è effettuato sia con strumenti elettronici che senza l'ausilio degli strumenti stessi.

3. Il trattamento dei dati personali deve essere effettuato nel rispetto dei principi previsti dagli articoli 18, 19, 20, 21 e 22 del Codice e con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato come indicato negli articoli 11, 12, 13, 14, 16 e 17 del Codice.

4. Il trattamento comprende, in particolare, le seguenti operazioni sui dati: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, cancellazione, distruzione, comunicazione, diffusione.

5. La definizione di trattamento ai sensi del Codice ricomprende sia una singola operazione che una serie di operazioni e si ha trattamento di dati anche quando le operazioni siano effettuate senza l'ausilio di strumenti elettronici, nonché riguardino dati non registrati in banche dati.

6. Oggetto del trattamento devono essere i soli dati essenziali per svolgere l'attività istituzionale, e le sole operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito.

7. I Responsabili del trattamento, con riferimento agli adempimenti di cui all'art. 11 del Codice, sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi.

8. Ai sensi dell'art. 3 del Codice, i responsabili sono tenuti a comunicare dati personali e/o sensibili ad altri Responsabili sia interni che esterni all'Azienda solo in caso di necessità, ovvero quando non sia possibile perseguire le stesse finalità con dati anonimi o aggregati che impediscano di identificare l'interessato.

9. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo che per eventuale conservazione, a norma di legge, dell'atto che li contiene.

10. I trattamenti di dati effettuati utilizzando le banche dati di diversi Titolari, sono autorizzati nelle sole ipotesi previste da espressa disposizione di legge o previa specifica autorizzazione da parte dell'Autorità Garante.

11. Sono consentite la comunicazione e la diffusione di dati personali, se richieste in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, del Codice per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

ART.25 –MODALITA' DI TRATTAMENTO DI DATI COMUNI

1. Il trattamento dei dati personali comuni è consentito solo per lo svolgimento dei compiti istituzionali, nei limiti stabiliti dalla legge e dai regolamenti.

2. Il suddetto trattamento è effettuato senza il consenso dell'interessato, che ha comunque il diritto di ricevere, in forma orale o per scritto, anche tramite affissione di appositi comunicati nei locali di accesso del pubblico, l'informativa prevista dall'art. 13 del Codice.

3. La comunicazione e la diffusione dei dati personali comuni ad altri soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da norme di legge o di regolamento. In mancanza, la comunicazione può essere effettuata quando sia comunque necessaria per lo svolgimento delle funzioni istituzionali, secondo le modalità previste dall'art. 19, comma 2, del Codice e le eventuali specifiche determinazioni del Garante.

4. La comunicazione e la diffusione dei dati personali comuni a soggetti privati o a soggetti pubblici economici è ammessa unicamente quando sia prevista da norme di legge o di regolamento.

5. I dati personali comuni devono essere trattati in modo lecito, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini non incompatibili con tali scopi.

6. I Responsabili del trattamento sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.

7. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.

ART.26 –MODALITA' DI TRATTAMENTO DI DATI SENSIBILI

1. Il trattamento dei dati personali sensibili, compresa la loro comunicazione, è consentito solo se autorizzato da espressa disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite ai sensi dell'art. 20 del Codice.

2. Nel caso si rilevi un trattamento di dati personali sensibili per il quale non esista una espressa disposizione legislativa che indichi la rilevante finalità di interesse pubblico, il Titolare del trattamento dovrà richiedere al Garante, in attesa della specificazione legislativa, l'attribuzione dello stesso tra quelli che perseguono rilevanti finalità pubbliche.

3. Nel caso in cui, invece, nella legge di riferimento è specificata la finalità di rilevante interesse pubblico ma non i tipi di dati che possono essere trattati e le operazioni eseguibili, il Titolare è tenuto a identificare e rendere pubblici i tipi di dati e di operazioni strettamente pertinenti e necessari, in relazione alle singole finalità perseguite.

4. I dati idonei a rivelare lo stato di salute e la vita sessuale non possono essere diffusi.

5. L'Azienda può trattare i dati personali sensibili con il limite dell'indispensabilità rispetto alle attività istituzionali che non possono essere realizzate mediante il ricorso a dati anonimi o a dati personali di diversa natura.

6. Il Responsabile del trattamento deve verificare, ogni volta ne ricorra la necessità, la congruità tra i dati richiesti e trattati e gli adempimenti di competenza. I dati che risultassero eccedenti non pertinenti e/o non necessari non possono essere utilizzati ma solo tenuti in archivio per il tempo previsto dalle leggi per gli archivi pubblici.

7. I dati contenuti in elenchi, registri, o banche dati tenute con l'ausilio di mezzi automatizzati, devono essere trattati con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altri sistemi che permettano di identificare gli interessati solo in casi di necessità come previsto nell'art. 22, comma 6, del Codice.

8. Il trattamento dei dati relativi alla salute ed alla vita sessuale devono avvenire con le tecniche di cui al precedente comma 7, anche quando tali dati non siano contenuti in elenchi, registri, o banche dati. Inoltre, devono essere conservati separatamente da ogni altro dato personale, trattato per finalità che non richiedono il loro utilizzo ai sensi di quanto disposto nell'art. 22, commi 6 e 7 del Codice.

9. L'utilizzo dei dati relativi alla salute ed alla vita sessuale non è consentito nell'ambito di test psico-attitudinali, volti a definire il profilo o la personalità dell'interessato.

10. Per il trattamento dei dati sensibili sono ammesse solo le operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti in occasione dell'attività di vigilanza, di controllo e ispettiva, esercitata anche per conto di altri soggetti.

11. La documentazione e/o la certificazione trasmessa ai soggetti richiedenti deve contenere esclusivamente le informazioni relative a stati, fatti, qualità personali richieste da leggi o da regolamenti, e strettamente necessarie al conseguimento delle finalità per le quali vengono acquisite.

ART.27 –MODALITA' DI TRATTAMENTO DI DATI GIUDIZIARI

1. Il trattamento di dati giudiziari è ammesso se indispensabile per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

2. Il trattamento dei dati giudiziari, compresa la loro comunicazione, è consentito solo se autorizzato da espressa disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite ai sensi dell'art. 20 del Codice.

3. Nel caso si rilevi un trattamento di dati giudiziari per il quale non esista una espressa disposizione legislativa che indichi la rilevante finalità di interesse pubblico, il Titolare del trattamento dovrà

richiedere al Garante, in attesa della specificazione legislativa, l'attribuzione dello stesso tra quelli che perseguono rilevanti finalità pubbliche

4. Nel caso in cui, invece, nella legge di riferimento è specificata la finalità di rilevante interesse pubblico ma non i tipi di dati che possono essere trattati e le operazioni eseguibili, il Titolare è tenuto a identificare e rendere pubblici, tipi di dati e di operazioni strettamente pertinenti e necessari, in relazione alle singole finalità perseguite.

5. I dati giudiziari contenuti in elenchi, registri, o banche dati tenute con l'ausilio di mezzi automatizzati, devono essere trattati con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altri sistemi che permettano di identificare gli interessati solo in casi di necessità come previsto nell'art. 22, comma 6, del Codice.

ART.28 –TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

1. Per trasferimento di dati personali si deve intendere, ai sensi degli artt. da 42 a 45 del Codice, ogni mero spostamento anche temporaneo di informazioni sia all'interno che all'esterno dell'ambito di titolarità del trattamento.

2. E' considerato trasferimento di dati personali all'estero anche la loro semplice momentanea allocazione su un server del titolare situato all'esterno del territorio nazionale.

3.I dati personali possono essere trasferiti fra gli Stati Membri dell'Unione Europea, dandone indicazione nell'informativa sul trattamento dei dati.

4. Al di fuori dei casi previsti dagli artt. 43 e 44 del Codice, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma e mezzo, di dati personali verso un Paese non appartenente all'Unione Europea è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato.

ART.29 –TRATTAMENTI PARTICOLARI DI DATI

1.Nei casi di attivazione di trattamenti di dati con modalità particolari tali da coinvolgere anche informazioni relative al personale dipendente (videosorveglianza, monitoraggio di posta elettronica e degli accessi ad internet ecc.) l'Azienda rimanda a specifiche policy atte a garantire il rispetto della normativa in tema di riservatezza dei dati personali nonché di quella a tutela del lavoratore dipendente.

ART.30 – USO DEGLI STRUMENTI DUI VIDEOSORVEGLIANZA - VIDEO MONITORAGGIO

1.L'installazione di apparecchiature di video-sorveglianza è autorizzata dal Titolare, previo accordo con le organizzazioni sindacali, solo quando ciò sia strettamente indispensabile per la sicurezza delle persone e delle attrezzature (controllo di corridoi, di sale di attesa, di spazi esterni, delle porte di accesso agli edifici) e non siano attuabili o sufficienti altre misure di sorveglianza.

2. Il trattamento dei dati personali con le apparecchiature di cui al comma 1 è effettuato nel rispetto della dignità e dell'immagine delle persone, delle norme a tutela dei lavoratori e delle prescrizioni del Garante.

3. Il Titolare fornisce al responsabile del trattamento le istruzioni necessarie sulle modalità di trattamento dei dati raccolti con le apparecchiature di video-sorveglianza, sulle misure di sicurezza da osservare, nonché sull'informativa da fornire agli utenti, agli operatori e alle altre persone che a qualsiasi titolo accedono agli spazi sorvegliati, in relazione alle finalità e alla tipologia del sistema di sorveglianza con l'adozione di specifiche policy.

4. L'attività di videomonitoraggio, che si distingue rispetto alle attività di videosorveglianza propriamente dette, ha particolari finalità, come ad es. quella relativa alla sorveglianza remota di pazienti ricoverati, per esclusive finalità di cura e tutela della salute**.**

5. Tale attività non prevede ordinariamente la registrazione delle immagini. L'attività di videomonitoraggio sarà indicata nell'informativa prestata al paziente nonché nell'informativa breve affissa nei locali interessati, e ad essa sarà prestato il consenso generale al trattamento dei dati per finalità di tutela della salute.

6.Potranno accedere alle immagini rilevate per le predette finalità solo i soggetti specificatamente autorizzati (es. personale medico e infermieristico).

7. Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione) ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente, le immagini idonee a rilevare lo stato non devono essere comunque diffuse (art. 22, comma 8, del Codice).

ART.31 – NOTIFICAZIONE E COMUNICAZIONI AL GARANTE

1. Ai sensi dell'art.37 del Codice è obbligo di notificare al Garante il trattamento dei dati personali specificati nel citato art.37, comma 1.

2. Il Garante può individuare con proprio provvedimento altri trattamenti rispetto a quelli già indicati nel suddetto art.37, comma 1, suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato in ragione delle relative modalità o della natura dei dati personali.

3. La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta.

4. Una nuova notificazione è richiesta in caso di cessazione di trattamenti previsti dall'articolo 37 del Codice o di mutamento di taluno degli elementi già comunicati nella prima notificazione od in quelle successive di variazione, nonché nel caso di nuovo trattamento ricompreso in una tipologia non precedentemente notificata.

5. La procedura di notificazione al Garante è coordinata a cura del RAP secondo le modalità indicate al comma 2 dell'articolo 38 del Codice stesso.

6. Ogni responsabile del trattamento è tenuto a fornire al RAP tutti gli elementi informativi necessari per effettuare la notificazione, nonché le comunicazioni di cui al successivo comma 7, con tutte le variazioni intervenute che incidono sulla relativa notificazione quale presupposto di legittimità del trattamento che viene effettuato.

7. Il RAP trasmette al Garante le comunicazioni previste dall'articolo 39, comma 1, del Codice.

ART.32 – CENSIMENTO DEL TRATTAMENTO DEI DATI - CETRA

1. L'Azienda predispone ed aggiorna un Censimento dei trattamenti (CeTra) dei dati personali che fanno parte del proprio patrimonio informativo, tenendo conto delle funzioni istituzionali assegnate a ciascuna struttura come da Regolamento di organizzazione vigente nel tempo, delle informazioni fornite a cura dei vari responsabili del trattamento, nonché con riferimento ai dati sensibili e giudiziari a quanto previsto nel regolamento regionale n. 6/R del 2013 – contenente l'elenco dei trattamenti dei dati applicabile alle aziende sanitarie.

2. L'individuazione dei trattamenti all'interno di ciascuna struttura consente in particolare la possibilità di designare gli incaricati del trattamento mediante la documentata preposizione della persona fisica ad una struttura per la quale è individuato l'ambito del trattamento consentito al personale assegnato alla struttura stessa.

3. Il CeTra è tenuto a cura del RAP, è soggetto ad aggiornamento periodico sulla base delle comunicazioni fornite dai vari responsabili che, in maniera autonoma ed automatica hanno l'obbligo di comunicare al RAP qualsiasi variazione di trattamento di dati e di personale assegnato.

ART.33 – INFORMATIVA

1. Il responsabile del trattamento, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, avvalendosi del personale incaricato, individuato a norma dell'art. 16 una completa informazione riguardo alle notizie indicate dall'articolo 13 del Codice.

2. Salvo quanto previsto nei commi 4 e 5, l'informativa di cui al comma 1 viene fornita, di norma, agli interessati mediante idonei strumenti quali:

- avvisi da affiggere in evidenza all'ingresso delle strutture dell'azienda, nelle sale d'attesa e negli altri locali di affluenza del pubblico;
- appositi moduli e depliant da consegnare agli interessati;
- apposite avvertenze inserite nelle lettere di affidamento di un determinato servizio o nei contratti.

3. Nell'informativa di cui al comma 2 è indicato il soggetto e l'eventuale sito della rete di comunicazione, presso cui l'interessato può rivolgersi per ulteriori e maggiori informazioni, anche al fine di consultare l'elenco aggiornato dei responsabili, nonché per esercitare i propri diritti.

4. Al personale dipendente, ai soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, agli specializzandi, ai tirocinanti, agli allievi ed ai docenti, ai volontari, agli operatori del servizio civile, comunque, ai soggetti che a qualsiasi titolo instaurano rapporti con l'Azienda, si deve provvedere ad un'idonea informativa ai sensi dell'art. 13 del Codice. Ai soggetti che hanno già instaurato rapporti con l'Azienda, i Responsabili del trattamento competenti devono provvedere a fornire l'informativa.

5. Alle ditte partecipanti a gare di forniture di beni o servizi o di affidamento di lavori, ai candidati di concorsi o di avvisi pubblici, l'informativa, viene resa in sede di pubblicazione dei relativi bandi, con l'indicazione del responsabile del trattamento dei dati relativi alle suindicate procedure. Ai soggetti che hanno già instaurato rapporti con l'Azienda, i Responsabili del trattamento competenti devono provvedere a fornire l'informativa.

6. In particolari situazioni, l'informativa può essere resa oralmente e, sempreché possibile, attestata per iscritto.

7. Le modalità per fornire agli interessati l'informativa di cui al presente articolo sono definite d'intesa tra il RAP e i responsabili del trattamento.

ART.34 – CONSENSO

1. Nei trattamenti dei dati personali idonei a rivelare lo stato di salute, effettuati per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato, l'Azienda organizza modalità atte a facilitare l'espressione del consenso da parte dell'interessato, secondo le indicazioni contenute negli articoli 81 e 82 del Codice.

2. In caso di incapacità di agire, ovvero di impossibilità fisica o di incapacità di intendere o di volere dell'interessato, il consenso di cui al comma1 viene prestato, rispettivamente, da chi esercita legalmente la potestà ovvero da un familiare, da un prossimo congiunto, da un convivente, o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato ai sensi dell'art. 82, comma 2, lett.a) del Codice.

3. Nel trattamento di dati finalizzato a scopi di ricerca scientifica, in campo medico, biomedico o epidemiologico l'Azienda organizza modalità atte a facilitare l'espressione del consenso secondo le indicazioni contenute nella relativa autorizzazione generale del Garante n.9 rinnovata, di norma annualmente, dallo stesso Garante.

4. Per il trattamento dei dati personali diversi di quelli di cui ai commi 1 e 3, non è necessario il consenso dell'interessato.

ART.35 – FASCICOLO SANITARIO ELETTRONICO E DOSSIER SANITARIO ELETTRONICO

1. Il fascicolo sanitario elettronico (FSE) e il dossier sanitario elettronico (DSE) sono trattamenti di dati effettuati tramite strumenti informatici di insiemi di dati e documenti sanitari riferiti logicamente ad un medesimo soggetto allo scopo di documentarne la storia clinica.

2. Si ha DSE qualora tale strumento sia costituito presso un organismo sanitario, al cui interno operino più professionisti in qualità di unico titolare del trattamento.

3. Si ha FSE in riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale.

4. Il trattamento di dati sanitari di cui al precedente comma 1, costituisce trattamento ulteriore e facoltativo rispetto al trattamento effettuato dal sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico per il quale l'interessato si rivolge ad esso.

5. Nell'eventualità di porre in atto trattamenti riferiti al FSE ed al DSE deve essere garantito il principio di autodeterminazione dell'interessato anche mediante la predisposizione di idonea ed adeguata informativa con acquisizione di un consenso espresso e specifico, anche per gli eventi clinici pregressi, di poter esercitare il diritto di "oscuramento" in modalità di "oscuramento dell'oscuramento", nonché deve essere garantito il rispetto degli adempimenti previsti in materia di protezione del dato dalle disposizioni vigenti in materia.

ART.36– COMUNICAZIONI E NOTIZIE SULLO STATO DI SALUTE DEGLI UTENTI

1. Le comunicazioni e le informazioni sulle specifiche patologie dell'interessato possono essere rese a quest'ultimo solo per il tramite del medico dell'Azienda competente in relazione ai provvedimenti organizzativi Aziendali, ovvero per il tramite del medico di fiducia dell'interessato da lui designato o del medico che ha prescritto il ricovero o gli accertamenti ai sensi dell'art. 84, comma 1, del Codice.

2. Il responsabile del trattamento dei dati personali può autorizzare per iscritto gli esercenti le professioni sanitarie diversi dai medici che, nell'esercizio dei propri compiti, intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato. L'autorizzazione è disposta in sede di designazione dei predetti esercenti quali incaricati al trattamento dei dati e ne individua i limiti, le modalità e le cautele ai sensi dell'articolo 84, comma 2, del Codice.

3. Nel caso l'interessato si trovi in stato di impossibilità fisica, di incapacità di agire, di incapacità di intendere e di volere, le comunicazioni e le informazioni di cui ai precedenti commi 1 e 2 sono rese a chi dimostri, anche mediante autocertificazione resa ai sensi dell'articolo 46 del D.P.R. 28.12.2000 n. 445, di esercitare legalmente la potestà ovvero di essere un prossimo congiunto, un familiare, un convivente, o, in loro assenza, il responsabile della struttura presso cui dimora l'interessato, ai sensi dell'art. 82, comma 2, lett.a) del Codice.

4. Le informazioni di cui ai commi 1 e 2 possono essere rese anche a familiari dell'interessato o a terzi, durante il suo ricovero o in sede di pronto soccorso, soltanto previo consenso scritto dell'interessato stesso, da acquisire preventivamente.

5. Le cartelle cliniche, i referti di pronto soccorso, i referti concernenti le prestazioni diagnostiche, le relazioni e le schede sanitarie, le certificazioni rilasciate da organismi sanitari, nonché qualsiasi altro documento contenente dati personali idonei a rivelare lo stato di salute, sottoscritti dalle persone competenti, in relazione alla vigente normativa e agli atti di organizzazione Aziendale, e redatti in forma intelligibile per l'interessato, sono consegnati in busta chiusa al medesimo ovvero a persona da lui delegata per iscritto, munita di documento di riconoscimento proprio e, anche in fotocopia, del delegante, dei quali dovranno essere annotati gli estremi.

ART.37 – ACCESSO ALLE LISTE DI ATTESA -

1. Per le finalità di cui al comma 8 dell'articolo 3 della legge 23 dicembre 1994, n. 724 e fatto salvo il diritto di accesso da esercitarsi ai sensi dell'art.41 del presente regolamento, l'interessato ha diritto a conoscere, anche tramite un proprio delegato da identificarsi come previsto all'art. 25, comma 5, il numero di posizione che occupa nelle liste delle prestazioni ambulatoriali, di diagnostica strumentale e di laboratorio, dei ricoveri ospedalieri e nelle altre liste di attesa, ma non può essere messo a conoscenza dei nominativi delle persone che lo precedono o che lo seguono nell'elenco.

2. Fuori dei casi di cui al comma 1, le informazioni sulle prenotazioni e sui relativi tempi di attesa sono fornite ai soggetti che vi abbiano interesse, a norma della L.241/90 e smi, con la salvaguardia del diritto alla riservatezza delle persone.

ART.38 – PROCEDURE ORGANIZZATIVE A TUTELA DELLA RISERVATEZZA IN AMBITO SANITARIO -

1. Presso tutti i presidi dell'Azienda, a cura del dirigente responsabile del presidio medesimo, sono adottate procedure, quali l'adozione di opportuna segnaletica per delimitare le distanze di cortesia, atte a garantire la riservatezza degli utenti in occasione di richiesta o fruizione di prestazioni sanitarie (prenotazioni, esami diagnostici, visite mediche, certificazioni, etc.) o amministrative (rimborsi, indennità, ecc.).

2. I dirigenti di presidio nonché i responsabili dei trattamenti sono tenuti ad adottare idonee misure atte a garantire che le informazioni sanitarie personali rese agli utenti verbalmente (chiamata dei pazienti, indagine anamnestica, elaborazione diagnostica, colloqui con familiari, ecc.) o tramite supporto cartaceo (documenti sanitari), non siano accessibili o percepibili da parte di terzi non espressamente autorizzati dagli interessati.

3. Le strutture ospedaliere possono fornire informazioni sui degenti, anche tramite il centralino telefonico, limitatamente alla loro presenza in ospedale e sulla loro collocazione all'interno della struttura, salvo che il degente chieda di non rendere nota la sua presenza.

4. Non possono essere esposti al pubblico, nei reparti o in altri locali, i nominativi dei pazienti ricoverati.

5. Il trattamento dei dati idonei a rivelare le convinzioni religiose non può avvenire in maniera sistematica e preventiva ma solo su richiesta dell'interessato o, qualora lo stesso sia impossibilitato, di un terzo legittimato quale ad esempio un familiare, un parente un convivente; si rinvia in merito ad una specifica policy.

6. Può essere data notizia, anche per via telefonica, circa una prestazione di pronto soccorso o meglio darne conferma. La notizia/conferma deve essere fornita ai soli terzi legittimati quali possono essere familiari, parenti, conviventi valutate le diverse circostanze del caso, nella consapevolezza che si tratta di verifica dagli esiti incerti. Le informazioni, trasmesse, comunque riguarderanno solo che è in atto o si è svolta una prestazione di pronto soccorso e non si devono risolvere in informazioni più dettagliate sullo stato di salute.

ART.39 – REDAZIONE DEGLI ATTI – PUBBLICITA' E TUTELA DELLA TRASPARENZA

1. I responsabili delle strutture organizzative che propongono una deliberazione o che adottano un provvedimento dirigenziale con il supporto tecnico dei relativi responsabili del procedimento verificano, alla luce dei principi di pertinenza e non eccedenza sanciti dal Codice, che l'inclusione nel testo e nell'oggetto di dati personali sia realmente necessaria per perseguire le finalità dell'atto stesso.

2. Devono essere privilegiate modalità di redazione degli atti che prevedono l'utilizzo di dati anonimi o non direttamente identificativi, quali codici o altri riferimenti se lo scopo cui l'atto è preordinato è ugualmente raggiungibile.

3. L'Azienda garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo delle deliberazioni o di altri atti, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati.

4. Per assicurare, comunque, la completezza delle deliberazioni/provvedimenti, i dati personali da escludere dalla pubblicazione sono inseriti in un apposito allegato all'atto che non viene pubblicato all'Albo rimanendo depositato agli atti della struttura proponente/adottante. Sull'allegato deve essere apposta la dizione "Riservato si sensi delle vigente norme per la tutela della riservatezza" e nella relativa delibera o provvedimento deve essere data evidenza che l'allegato non è pubblicato all'Albo per la tutela della riservatezza.

ART. 40 -OBBLIGHI DI TRASPERENZA

1. L'azienda assolve agli obblighi di legge in materia di trasparenza, quale livello essenziale delle prestazioni concernenti diritti civili e sociali ai sensi dell'art.117, lettera m) della Costituzione, con la pubblicazione sul proprio sito internet istituzionale dei dati di cui al D.Lgs 33/2013 e smi, nel rispetto delle linee guida impartite dal Garante per la privacy in materia.

2.Ogni cittadino-utente, portatore di quell'interesse nel cui perseguimento e nella cui tutela va ricercata la stessa ragion d'essere di ogni Pubblica Amministrazione, è posto in questo modo nella condizione di poter agevolmente verificare: quali trattamenti potranno essere effettuati con i suoi dati personali, una volta conferiti; quali strutture sono autorizzate a porre in essere i vari tipi di trattamento previsti; qual è l'organigramma privacy aziendale, ossia la rete dei soggetti individuati dal Titolare medesimo quali Responsabili (interni ed eventualmente anche esterni) delle operazioni di trattamento.

ART. 41 -ESERCIZIO DEI DIRITTI DI CUI ALL'ART 7 DEL CODICE

1. Per i diritti dell'interessato in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni previste dagli articoli 7, 8, 9 e 10 del Codice.

2. La richiesta per l'esercizio dei diritti di cui al comma 1 può essere fatta pervenire:

- direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia od anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso (es. la conoscenza personale);
- tramite altra persona fisica od associazione (es. sindacato, associazione di tutela, ecc.), a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento d'identità del sottoscrittore;
- tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;
- se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica a ciò legittimata in base ai rispettivi statuti od ordinamenti.

3. L'interessato può presentare od inviare la richiesta di cui al comma 2:

- al responsabile del trattamento, che conserva e gestisce i dati personali dell'interessato;
- al protocollo generale dell'Azienda che ne curerà l'inoltro al responsabile del trattamento.

4. La richiesta per l'esercizio dei diritti di cui al comma 1 può essere esercitata dall'interessato solo in riferimento alle informazioni riguardanti la propria persona e non si estende ai dati relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano. Nel caso che i dati relativi al

richiedente siano intrecciati con quelli di terzi al punto tale da essere incomprensibili o snaturati nel loro contenuto, se privati di alcuni elementi o scomposti rispetto alla loro originaria collocazione, il responsabile del trattamento autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso previste dall'art.41 del presente regolamento.

5. Per agevolare l'esercizio dei diritti da parte dell'interessato, è predisposta apposita modulistica.

6. Il riscontro alle richieste degli interessati deve essere fornito entro quindici giorni dalla data di ricezione. Se le operazioni necessarie per l'integrale riscontro sono di particolare complessità ovvero ricorre altro giustificato motivo, il riscontro può essere fornito entro trenta giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato.

7. I diritti riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

ART. 42 - DIRITTO DI ACCESSO ALLA DOCUMENTAZIONE -

1. Nel caso in cui nel corso della procedura di accesso ai documenti amministrativi venissero in evidenza problematiche connesse alla tutela della privacy di soggetti terzi, di cui ai seguenti commi 3 e 4, sarà compito del responsabile del trattamento, valutare caso per caso la possibilità di esercitare il diritto di accesso.

2. Salvo quanto previsto all'art. 39 e fatti salvi gli atti sottratti all'accesso per norma di legge o di regolamento, l'Azienda garantisce il diritto di accesso alla documentazione amministrativa ai sensi degli articoli 59 e 60 del Codice, nonchè dell'articolo 22 della L. 241/90 e smi.

3. Nel caso l'istanza di accesso riguardi documentazione contenente dati comuni o sensibili di terzi, salvo quanto previsto al comma 4, l'accesso è limitato alla sola visione dei dati la cui conoscenza sia necessaria per curare o difendere un proprio interesse giuridico, nel rispetto dei principi di pertinenza e di non eccedenza dei dati da visionare rispetto alle finalità per le quali è consentito l'accesso stesso.

4. Qualora l'istanza di accesso riguardi documenti contenenti dati idonei a rivelare lo stato di salute o la vita sessuale di un terzo, l'accesso è consentito a condizione che ciò si renda necessario per far valere o difendere in sede giudiziaria una situazione giuridicamente rilevante di rango almeno pari ai diritti del terzo, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso stesso ai sensi dell'art. 60 del Codice.

ART. 43 - DIRITTO DI ACCESSO CIVICO -

1.Nel caso in cui nel corso della procedura di accesso civico ai sensi del D.Lgs 33/2013 e smi, venissero in evidenza problematiche connesse alla tutela della privacy di soggetti terzi, l'accesso civico generalizzato deve essere rifiutato laddove possa arrecare un pregiudizio concreto alla protezione dei dati personali in conformità con la disciplina legislativa in materia.

2.Il responsabile del trattamento dei dati interessato dall'accesso civico generalizzato dovrà operare la valutazione caso per caso al fine di verificare la sussistenza o meno del pregiudizio nel rispetto della normativa di settore, in particolare delle Linee Guida adottate dall'Autorità Nazionale Anticorruzione d'intesa con il Garante di cui alla delibera n. 1309 del 28/12/2016.

ART. 44 - FORMAZIONE -

1. L'Azienda, organizza, di norma, nell'ambito del piano annuale di formazione del personale, interventi di formazione e aggiornamento in materia di tutela della riservatezza e protezione dei dati personali, finalizzati alla conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni ai dati stessi.

2.L'intervento formativo predisposto dall'Azienda ricomprende anche le azioni generali di informazione e formazione attivate nell'ambito del Sistema Aziendale Privacy (es. "Il Cruscotto per la Privacy quale strumento esclusivamente on-line).

ART. 45 - LA SEMPLIFICAZIONE

1. L'Azienda, considerando la semplificazione quale fattore principale su cui far leva per il perseguimento dei fondamentali principi di buon andamento, efficienza, efficacia ed economicità dell'attività amministrativa, promuove azioni e progetti volti alla semplificazione dei processi e delle procedure interne rivolti all'esecuzione di adempimenti normativi e regolamentari in materia di protezione dei dati personali.

ART. 46 - ABROGAZIONI-

1. Sono abrogate tutte le disposizioni aziendali in contrasto con quelle previste dal presente regolamento.

ART. 47 - RINVIO ED ADEGUAMENTO-

1. Per quanto non previsto dal presente regolamento si applicano le disposizioni contenute nel Codice e nei provvedimenti emanati dal Garante, nonché dalla Regione Toscana.

2. Gli eventuali interventi del legislatore nazionale e regionale successivi all'entrata in vigore del presente regolamento, di modifica del quadro normativo sulla riservatezza e protezione dei dati personali, producono un automatico adeguamento del presente regolamento con successivo e necessario aggiornamento con le modalità previste per l'approvazione delle procedure aziendali.

3. Il presente regolamento sarà oggetto di necessaria revisione con l'avvenuta applicabilità del Regolamento Europeo pubblicato sulla Gazzetta Ufficiale della UE del 04/05/2016.

* * * * *